FORUM FOR AFRICAN WOMEN EDUCATIONALISTS ZIMBABWE (FAWEZI)
BINDURA UNIVERSITY OF SCIENCE EDUCATION (BUSE)

TERMS OF REFERENCE

Information Technology (IT) Software Consultant: Design, Development, Pilot and Handover of the Gender-Transformative Digital (GTD) Hub

1. GENERAL INFORMATION

Services Required	An IT software consultant to design, develop, test, pilot, deploy and hand over the Gender-Transformative Digital (GTD) Hub, a secure, mobile- and web-accessible platform for gender-based violence (GBV) reporting, referral, mentorship, peer support, learning and advocacy in Science, Technology, Engineering and Mathematics (STEM) faculties of Zimbabwean higher education institutions (HEIs).
Project/Programme Title	Promoting Gender Responsiveness in Higher Education: An Integrated Mentorship Network and Community-Centred Support Hub Approach (PROGEN-Hub for STEM)
Funder	Sexual Violence Research Initiative (SVRI) Research Grant
Implementing Partners	FAWEZI (lead organisation) and BUSE
Post Title	IT Software Consultant (GTD Hub Developer)
Type of Contract	Individual Consultant (lump-sum, deliverable-based)
Duty Station	Bindura (BUSE), with remote working and coordination with FAWEZI in Harare
Expected Places of Travel	Local: selected participating HEIs for co-design workshops, the pilot and training
Duration	40 working days commencing on the date the contract is signed in December 2026 and ending no later than 29 January 2027 (37 working days of consultant input and a three-day design review by the partners), followed by a three-month post-launch support period
Expected Start Date	On the date the contract is signed, in December 2026

2. BACKGROUND / PROJECT DESCRIPTION

Gender-based violence and gender inequality remain persistent in Zimbabwean higher education and are particularly acute in STEM faculties. Institutional responses tend to be fragmented, with policies and mentorship programmes run in silos, and HEIs have yet to harness digital innovation in gender-transformative programming in STEM.

The PROGEN-Hub for STEM project, led by FAWEZI in partnership with BUSE and funded by SVRI, responds with an integrated mentorship network and community-centred support hub across eleven HEIs in Zimbabwe's ten provinces. The project runs for 18 months, from 1 March 2026 to 31 August 2027. It aims to enhance gender responsiveness and reduce GBV in STEM faculties through co-developed mentorship networks and digital support hubs that enable sustainable institutional transformation.

At the centre of the project is the GTD Hub, a participatory digital platform co-designed with STEM students and staff. The Hub will allow users to identify risk factors, report GBV safely and anonymously, access psychosocial support and confidential referral, take part in mentorship and peer forums, use learning resources such as the Gender-Responsive Mentorship and Change Champions Toolkit, join advocacy campaigns and give ongoing feedback. The Hub is both a service for students and staff and a research instrument that supports the project's monitoring and evaluation (M&E).

The GTD Hub is distinct from the PROGEN Hub. The PROGEN Hub is the project's institutional mechanism for coordination, accountability and policy reform across the participating HEIs. It is made up of people, structures and processes, not software. The GTD Hub is the digital platform for reporting, referral, mentorship and engagement that supports the work of the PROGEN Hub and the participating HEIs. This assignment covers the design, development, pilot and handover of the GTD Hub only.

The project team has prepared a Technical Paper (Guidance for Software Developers, October 2026) that sets out the users, functional and non-functional requirements, recommended architecture, data management, security and safeguarding requirements, delivery approach and acceptance criteria for the Hub. The Technical Paper forms part of these Terms of Reference (TOR), and the consultant is expected to follow it.

FAWEZI and BUSE therefore seek the services of a qualified IT software consultant to build and launch the GTD Hub as a low-cost, open-source Progressive Web App (PWA), delivered first as a minimum viable product (MVP), then piloted, rolled out to all eleven HEIs and handed over to the partners.

3. OBJECTIVES

The overall objective of the assignment is to deliver a secure, accessible, low-bandwidth and sustainable GTD Hub that FAWEZI and BUSE can jointly own and maintain after the project. The specific objectives of the assignment are to:

i. Validate the requirements of the GTD Hub with students, staff, mentors and partners across the eleven participating HEIs;
ii. Design and develop an MVP covering the essential modules: identity and access; safe and anonymous GBV reporting; referral and psychosocial support directory; mentorship matching; peer forums and support groups; resource library and learning modules; feedback, surveys and M&E dashboards; and administration;
iii. Build security, privacy and safeguarding into the design, in line with Zimbabwe's Cyber and Data Protection Act [Chapter 12:07] of 2021 and international good practice;
iv. Pilot the Hub with about 100 participants in sample HEIs, refine it and roll it out to all eleven HEIs; and

v. Hand over the source code, documentation and skills to designated FAWEZI and BUSE information and communication technology (ICT) staff.

4. SCOPE OF WORK

The consultant shall design, build, test, pilot, deploy and hand over the GTD Hub in line with the Technical Paper, working iteratively in three short development sprints with a co-design group of students, staff, mentors and pilot users. The specific tasks to be performed by the consultant are to:

- **Inception and requirements validation:** hold kick-off meetings with FAWEZI, BUSE and the BUSE ICT Lead to align understanding and expectations; consult key stakeholders to validate the requirements; review the project proposal, baseline findings and the Technical Paper; and recommend a hosting arrangement for the project team's decision;
- **Co-design and wireframing:** facilitate, with the project team, co-design workshops and prototype testing with students, staff and mentors, including women, students with disabilities, lesbian, gay, bisexual, transgender, queer, intersex and asexual (LGBTQIA+) students and rural students; and produce wireframes or clickable prototypes of all key user journeys, a system architecture diagram, a data-flow diagram and a requirements and design document, and present them to FAWEZI and BUSE for a three-day design review and approval;
- **Development:** once the design has been approved in writing, build the MVP in three development sprints of two to three working days each as a modular web application and PWA using an open-source stack (Python/Django and PostgreSQL, or a justified alternative), with role-based access scoped by institution, a separate encrypted store for GBV case data, a quick-exit button, low-data pages and accessibility in line with the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA. Sprint 1 shall cover user registration and login, user roles and permissions, database set-up, anonymous GBV reporting and a basic reporting dashboard; Sprint 2 the mentorship matching module, peer support discussion forums, the resource repository and document library, and referral pathway management; and Sprint 3 analytics and dashboards, KoboToolbox integration, email and short message service (SMS) notifications, performance optimisation and a basic administration panel;
- **Reporting, referral and consent workflow:** configure the Hub to support the end-to-end reporting, referral and consent workflow set out below, and document it as a workflow diagram in the requirements and design document for the project team's approval;
- **Integration:** integrate the Hub with KoboToolbox for surveys and an SMS and email gateway for one-time passwords (OTPs) and notifications; and provide de-identified, aggregated exports or reporting views for Power BI or Apache Superset;
- **Internal quality assurance (QA) and security testing:** before the pilot, apply the Open Worldwide Application Security Project (OWASP) Top 10 and Application Security Verification Standard; carry out unit, integration, role-based access, usability, performance, privacy and security testing, using fictional cases only; and resolve all critical and high-severity findings and prepare, with the project team, a security incident-response plan before launch;
- **Pilot deployment and monitoring:** deploy the Hub to sample HEIs and support the training of case handlers, moderators and pilot users; then monitor the pilot and collect feedback with the M&E team, and report on pilot metrics;
- **Refinement and optimisation:** fix defects and make improvements based on the pilot findings, and prepare a refined release;
- **Full deployment:** configure and onboard all eleven HEIs; and set up development, staging and production environments, encrypted backups and uptime monitoring;

- **User adoption and training:** support user adoption across the eleven HEIs, including the online training of 150 Gender-Transformative Champions and the training of designated FAWEZI, BUSE and HEI ICT staff;
- **Documentation and handover:** deliver user guides and technical documentation, and transfer the source code repository, domain and hosting credentials to the partners; and
- **Post-launch support:** provide defect fixes and security updates for three months after launch at no additional cost.

The consultant shall have no access to live data by default. Where access is needed for technical support, it must be approved in advance and in writing by the BUSE ICT Lead and the Lead Researcher, limited to the minimum data and time needed, supervised where possible and logged, and the project team will review the access logs.

The Hub shall support the following end-to-end workflow, from submission to action. The final pathways, roles and response times will be confirmed by the project team and each participating HEI during co-design.

- Submission: a user submits a report anonymously or with contact details, chooses whether to consent to referral, and is shown support options, emergency contacts and what will happen next;
- Receipt and triage: the report is routed securely to the authorised case handler at the user's institution, who acknowledges it and assesses which pathway applies;
- Information-only pathway: where the user seeks information or support only, the user is given self-help resources, the support directory and helpline contacts, and no further action is taken without the user's request;
- Referral pathway: where the user consents, the case handler refers the case to psychosocial, medical, legal or other support services. Identifiable information is shared only with the user's informed and recorded consent, and only to the extent needed for the referral;
- Institutional-action pathway: where the user wishes to make a formal complaint, the case handler passes the case to the HEI's gender desk or designated office, which handles it under the HEI's own GBV policy and disciplinary procedures, and the outcome is recorded;
- Emergency-escalation pathway: where a report indicates an immediate risk to life or safety, the system immediately alerts the designated safeguarding focal person, who acts under the agreed safeguarding escalation protocol, and alerts a back-up contact if the alert is not acknowledged within one hour. Any sharing of information without consent is limited to what that protocol and the law permit; and
- Closure and feedback: the case handler records the actions taken and closes the case, the user is told the outcome where contact details were given, and only de-identified, aggregated data flow to the M&E dashboards.

The system shall record and route reports and prompt users and case handlers, but it shall not decide which pathway applies or what action is taken. All case-management decisions, including triage, referral, escalation and closure, shall be made by authorised personnel designated by the participating HEIs and the partners. Users may withdraw consent to referral at any time, and the system shall record each consent given or withdrawn.

5. EXPECTED DELIVERABLES

a) Inception report detailing the methodology, a detailed work plan and the recommended hosting arrangement;

b) Requirements and design document, including wireframes or prototypes of all key user journeys, a system architecture diagram, a data-flow diagram, the data model and a diagram of the reporting, referral and consent workflow, reviewed by FAWEZI, BUSE, SVRI and selected HEIs and approved in writing by FAWEZI and BUSE before software development begins;
c) MVP deployed in a pilot environment, with source code in a partner-owned repository and the results of testing and the security review;
d) Pilot report and refined release, including pilot metrics and the defects resolved; and
e) Production release rolled out to all eleven HEIs, with user guides, technical documentation and a training and handover report.

Approval of the requirements and design document is a formal milestone. FAWEZI, BUSE, SVRI and selected HEIs will review the prototypes and diagrams, and the consultant shall address their feedback. Software development shall not begin until FAWEZI and BUSE have confirmed the approval in writing. The partners will complete the review within three working days. The review period is included in the 40-working-day timeframe but does not count towards the consultant's 37 working days of input.

Table 5.1: Deliverables schedule

No.	Deliverable	Number of working days (consultant input)
1	Inception report	4 days
2	Requirements and design document	8 days
3	MVP in the pilot environment, with source code and test and security review results	9 days
4	Pilot report and refined release	9 days
5	Production roll-out, documentation and handover	7 days
	Total	**37 days**

6. INSTITUTIONAL ARRANGEMENTS FOR MANAGEMENT OF THIS CONSULTANCY

The partners will support the consultant's engagement with HEIs, arrange co-design workshops, pilot sessions and training, and provide access to relevant project documents.

The roles of the partners in oversight and decision-making are as follows:

- FAWEZI, as lead organisation, holds overall responsibility for the project and this assignment, contracts and pays the consultant, approves deliverables jointly with BUSE and leads the coordination, accountability and policy reform work of the PROGEN Hub;
- BUSE leads the technical build of the GTD Hub, supervises the consultant and provides technical oversight through the Lead Researcher, the BUSE ICT Lead and the project Data Scientist, approves deliverables jointly with FAWEZI and co-owns the platform after handover;
- SVRI, as funder, provides grant oversight in line with the grant agreement, receives progress reports and is consulted on key design and safeguarding decisions, and takes part in the design approval milestone; and
- Each participating HEI retains authority over GBV reports, case management, safeguarding and disciplinary matters involving its students and staff, acting through its gender desk and designated

focal persons under its own policies. HEIs nominate case handlers and moderators, take part in co-design, review of designs and the pilot, and confirm the referral pathways configured for their institution.

Under the overall supervision of the Lead Researcher, Dr Jeffrey Kurebwa (BUSE), working with the FAWEZI project coordinator, the consultant will be responsible for the quality of the software, documentation and training delivered under these TOR. The consultant will consult the youth advisory board on content and features, and the university gender desk coordinator on reporting pathways. The key technical decisions listed in Section 12 of the Technical Paper, such as ownership and hosting, case-handler roles, data retention and the safeguarding escalation protocol, must be confirmed in writing by the project team.

The GTD Hub supports institutional processes but does not replace them. Neither the platform nor the consultant shall hold any governance, safeguarding, disciplinary or decision-making authority. The system shall not make automated decisions on reports, referrals, cases or sanctions; all such decisions rest with authorised personnel designated by the partners and the participating HEIs. The consultant's role is limited to the technical design, development, testing, deployment, handover and support of the platform.

7. TIMEFRAME

The consultant is expected to complete the assignment within 40 working days commencing on the date the contract is signed in December 2026 and ending no later than 29 January 2027, covering inception, co-design, development, testing, the pilot, roll-out, training and handover, followed by a three-month post-launch support period. The 40 working days comprise 37 working days of consultant input and a three-day design review by FAWEZI and BUSE, as specified in Section 5. The engagement of the service provider, covering advertising, evaluation, interviews and contract signing, is expected to take ten working days before the contract is signed and is not part of the assignment. The phases, activities and working days are set out in Table 7.1. Hosting and expansion costs are budgeted separately by the project and are not part of the consultant's fee.

Table 7.1: Implementation timeline

Phase	Activities	Working days
Inception and requirements validation	Kick-off meetings, document review and stakeholder consultations	4
Co-design and wireframing	Co-design workshops, wireframe and prototype development, and the requirements and design document	8
Design review and approval	Review and written approval of the design by FAWEZI and BUSE (partners' review)	3
MVP development: Sprint 1	User registration and login; user roles and permissions; database set-up; anonymous GBV reporting; basic reporting dashboard	2
MVP development: Sprint 2	Mentorship matching module; peer support discussion forums; resource repository and document library; referral pathway management	3
MVP development: Sprint 3	Analytics and dashboards; KoboToolbox integration; email and SMS notifications; performance optimisation; basic administration panel	2
Internal QA and security testing	Testing and remediation of findings	2
Pilot deployment	Deployment to sample HEIs and training of pilot users	3
Pilot monitoring	Feedback collection and monitoring	3
Refinement and optimisation	Bug fixes and improvements	3
Full deployment	Roll-out to all eleven HEIs	2
User adoption and training	Training of Gender-Transformative Champions and ICT staff	3
Documentation and handover	Documentation and transfer of the source code, accounts and credentials	2
Total		**40**

8. IMPACT OF THE RESULTS

The assignment will give FAWEZI, BUSE and the eleven participating HEIs a safe, trusted and sustainable digital platform that strengthens GBV reporting pathways, connects survivors to support services, scales mentorship and peer networks in STEM and generates real-time data for the project's evaluation and policy influence. The Hub is intended to remain an enduring platform after the project and to be shared with about 100 institutions, non-governmental organisations (NGOs) and government bodies during the replication phase.

9. QUALIFICATIONS AND EXPERIENCE

Education:

The consultant must have the following minimum qualifications:

- A bachelor's degree in Computer Science, Software Engineering, Information Technology or a related field; a master's degree is an advantage; and
- Relevant certifications in secure software development, cloud computing or information security will be an advantage.

Experience:

- At least five years' relevant experience in full-stack web application development, with at least three production systems delivered;
- Demonstrated experience with Python/Django or an equivalent framework, PostgreSQL, Representational State Transfer (REST) application programming interfaces (APIs) and responsive or Progressive Web Apps;
- Demonstrated experience in building systems that handle sensitive personal data, including role-based access control, encryption and audit logging;
- Experience in applying OWASP secure-development practices and in organising vulnerability scanning and security reviews;
- Experience in designing low-bandwidth, mobile-first and accessible applications for users in low-resource settings;
- Experience with Git, Docker and automated continuous integration (CI) testing;
- Experience with integrations such as KoboToolbox, SMS gateways and data dashboards (Power BI or Apache Superset) is an advantage; and
- Experience in user-centred or participatory design with non-technical users.

Other Experience:

- Experience in developing platforms for GBV response, health, case management or the higher education sector is a strong advantage;
- Familiarity with Zimbabwe's Cyber and Data Protection Act and with research ethics requirements;
- Experience of trauma-informed or safeguarding-sensitive design;
- Experience with Flutter for cross-platform mobile apps is an advantage;
- Knowledge of the socio-cultural context of Zimbabwean HEIs is strongly desired; and
- Ability to work with multi-disciplinary teams, including researchers, M&E staff, students and ICT staff.

Competencies:

Functional Competencies:

- Strong software architecture, coding, testing and documentation skills;
- Ability to translate user needs into clear, workable features;
- Ability to train and transfer skills to non-specialist users and ICT staff; and
- Good project management skills, with the ability to deliver to agreed timelines.

Corporate Competencies:

- Promote the highest standards of ethics, integrity and confidentiality;
- Demonstrate gender sensitivity and respect for diversity and inclusion;
- Commit to safeguarding and a survivor-centred approach;

- Support creativity and innovation; and
- Share knowledge and support a culture of learning.

Language:

- An excellent command of written and spoken English is required; working knowledge of Shona or Ndebele is an advantage.

10. PAYMENT MILESTONES AND AUTHORITY

The consultant shall submit an all-inclusive, lump-sum financial proposal. The term "all-inclusive" means that all costs (professional fees, communications, data, equipment, software licences, consumables, etc.) that the consultant may incur in completing the assignment are included in the proposed fee. The financial proposal shall be submitted together with the technical proposal. The project will arrange and cover local travel to HEIs for co-design workshops, the pilot and training in line with its budget.

Payments will be released on submission of an invoice indicating the deliverables achieved, once these have been verified and approved by the Lead Researcher (BUSE) and FAWEZI, according to the following schedule:

Payment Instalment	Deliverable	Approval should be obtained from	Payment percentage
1st Instalment	Inception report; requirements and design document, approved at the design approval milestone	Lead Researcher (BUSE) and FAWEZI	20%
2nd Instalment	MVP deployed in the pilot environment, with source code in the partner-owned repository and test and security review results	Lead Researcher (BUSE) and FAWEZI	40%
3rd Instalment	Pilot report and refined release; production roll-out to all eleven HEIs; user guides, technical documentation and handover training report	Lead Researcher (BUSE) and FAWEZI	40%

11. INTELLECTUAL PROPERTY, CONFIDENTIALITY AND SAFEGUARDING

- All source code, designs, documentation, data and accounts produced under this assignment will be jointly owned by FAWEZI and BUSE, and the source code will be released under an open-source licence agreed by the project team;
- The source code must be kept in a repository owned by the partners from the start, and domains, hosting and third-party service accounts must be registered in the partners' names;
- The consultant shall sign a confidentiality agreement and the project's safeguarding code of conduct, and complete the required safeguarding and research ethics training before receiving access to the platform;
- The Hub must apply least-privilege, role-based access controls, so that each user, case handler, moderator and administrator sees only the data needed for their role and institution, with multi-factor authentication for all staff and administrator accounts;
- All personal and case data must be encrypted in transit, using Transport Layer Security (TLS) 1.2 or higher, and at rest, including backups, with encryption keys controlled by the partners;

- The Hub must keep tamper-evident audit logs of all access to and changes to case data, including any access by the consultant or system administrators, and these logs must be retained and available for review by the project team;
- The Hub must collect only the personal data needed for each function, allow anonymous reporting, keep case data separate from M&E data and apply the data retention and deletion periods agreed by the project team;
- Only fictional data may be used in development, testing and staging environments, real data must never be copied into these environments, and no participant may be asked to disclose real experiences during testing; and
- Any safeguarding concern or disclosure, suspected data breach or security incident that comes to the consultant's attention must be reported to the designated safeguarding focal person and the project team immediately, and in any case within 24 hours, in line with the incident-response plan. The consultant shall help to contain a security incident without delay, submit a written incident report within 72 hours and support the partners in meeting their notification duties under the Cyber and Data Protection Act. The consultant shall not investigate a safeguarding concern or contact the people involved.

12. HOW TO APPLY

Interested consultants should submit the following documents, combined into one Portable Document Format (PDF) file, to applications@fawezi.org by 25/11/26 1300Hrs C.A.T:

- Curriculum vitae (CV), including the contact details (email and telephone number) of at least three professional references;
- Cover letter confirming interest and availability for the assignment;
- Technical proposal demonstrating a full understanding of these TOR, with the proposed approach, methodology, technology stack and work plan;
- Portfolio with links to, or demonstrations of, at least two comparable systems the consultant has delivered; and
- Financial proposal: an all-inclusive lump-sum fee, broken down by deliverable.

Application Evaluation Process:

Applications will be evaluated using the cumulative analysis (weighted scoring) method. The contract will be awarded to the consultant whose offer is responsive, compliant and acceptable, and has received the highest combined score on the technical and financial criteria, weighted at 70% (technical) and 30% (financial). Only consultants obtaining a minimum of 70 of the 100 obtainable points in the technical evaluation will be considered for the financial evaluation. The lowest-priced financial proposal will receive the maximum financial score, and other proposals will be scored in inverse proportion to their price.

Technical Evaluation Criteria:

Criterion	Maximum points
Relevant academic qualifications and certifications	10
Experience in full-stack web development, PWAs and system integrations	25
Experience with sensitive-data systems, security and safeguarding	20
Technical proposal: understanding of the TOR, approach and methodology	30
Work plan and feasibility within the timeframe	15

Criterion	Maximum points
Total	**100**